7

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on line 15 of page 2 beginning with "A consumer desiring to make... with the following replacement paragraph.

B1

A consumer desiring to make payments for goods or services purchased at a retail location would typically present his/her credit or debit card to a representative of the merchant at the check out counter. The representative at the check out counter would swipe the card across a card reader which is typically attached to, or part of the processing terminal. Once the card is swiped, information associated with the transaction is transmitted via a private network maintained by private network operators, such as FIRST DATA CORP. ~~First Data Corp.~~, to a server associated with the private network. The private network server in turn sends information associated with the transaction to a server associated with the bank issuing the card (the issuing bank), again through a private network maintained by the private network operator. The issuing bank then sends back authorization for charging the card to the server maintained by the private network operator, which in turn sends the authorization to the retail location.

Please replace the paragraph beginning on line 26 of page 4 beginning with "It should be clear that the use of... with the following replacement paragraph.

B2

It should be clear that the use of existing card processing terminals requires a merchant to make a large initial investment in the purchase of various services and equipment in addition to the card processing terminal, such as application fees, setup fees, reprogramming fees, a receipt printer and/or a local host computer connected to the card processing terminal and/or a printer. Moreover, there are additional costs associated with leasing the communication lines from private network operators, such as FIRST DATA CORP. ~~First Data Corp~~. Leasing the equipment is also an option for merchants. However, leasing requires an on-going expense for the merchant in terms of the cost of the lease and adds to the overhead costs associated with operating a business. Furthermore, existing private network operators typically require multi-year contracts from merchants desiring to provide credit card processing facilities at their retail locations. Moreover, most card processing terminals currently in use that require a local host computer system for operation require some kind of custom software in order for them to be properly integrated with the host computer. B2

Please replace the paragraph beginning on line 13 of page 13 beginning with "The transaction processing device 40 of FIGURE 4 may ... with the following replacement paragraph.

B3 The transaction processing device 40 of FIGURE 4 may be used by these SOHO type businesses because device 40 does not need to connect to a private network, which is controlled by private network operators like FIRST DATA CORP. ~~First Data Corp.~~, but can instead communicate securely over a public network, such as the Internet, which is more accessible and cheaper to use. Thus, the SOHO type businesses do not need to sign multi-year contracts which data processor, banks and/or private network operators typically require for accessing the authorization networks and/or for purchasing or leasing the equipment. Moreover, the transaction processing device 40 of FIGURE 4 need not be manually provisioned or configured with the help of a representative of the data processor/bank thereby reducing the cost of installing the transaction processing device.

Please replace the paragraph beginning on line 15 of page 19 beginning with "FIGURE 7B shows a schematic diagram..." with the following replacement paragraph.

B4 FIGURE 7B shows a schematic diagram of the preferred embodiment cryptographic services 702 of the configuration server. Cryptographic services 702 facilitate secure provisioning and configuration of the transaction processing device. The physical security ~~702~~ 709 of the server provides physical protection against compromising the system, for example, by malicious third parties who might want to alter information in the associated databases or extract the various sensitive key sets utilized in the system. Physical security may also be provided by physically securing the location of the server. Each server has an ID associated with it. The ID 713 is preferably stored in the cryptographic services 702. The ID 713 of the server is preferably unique. In the preferred embodiment, the server's unique ID 713 cannot be altered or changed after it has been created. Also, in the preferred embodiment

B4

a key pair 714 associated with each server is internally generated in the server in order to ensure that it has not been altered or compromised during the manufacturing process. The cryptographic services 702 of the configuration server also has a copy 715 of the server certificate 708. In the preferred embodiment of the present invention, cryptographic services 702 also includes one or more cryptographic algorithms 717, such as RSA, DES, triple DES, elliptic curve and/or the like, one or more hashing algorithms 719, such as SHA1, MD5, and/or the like. If desired, these cryptographic algorithms and/or hashing algorithms could be implemented in hardware. Moreover, a cryptographic accelerator 718, such as a large modulus and exponentiation computation hardware, could be utilized to improve the overall performance of the cryptographic services. The cryptographic services 702 also include a terminal certificate database 720, which is capable of storing certificates associated with terminals. Moreover, cryptographic services 702 also preferably includes a merchant and user certificate database 721 which may be used to store merchant certificates, if desired. Merchant certificates and user certificates may be utilized in place of or in addition to user names and passwords for access control to add an additional layer of security. Such certificates may be issued for example by certificate manager 618 of FIGURE 6 or may be issued by trusted third party organizations, such as banks, government agencies, certifying authorities and/or the like.

Please replace the paragraph beginning on line 8 of page 22 beginning with "In the preferred embodiment, in step 905 the terminal..." with the following replacement paragraph.

B5

In the preferred embodiment, in step 905 the terminal authenticates itself to the configuration server, for example, by signing some data with the private key of the terminal's key pair. This signature is verified by the configuration server by using the public key of the terminal's key pair and comparing the signed data to ensure that it was signed by the corresponding private key which is only known to the terminal. In step 906 the terminal preferably encrypts the identifying token, and transmits the encrypted token to the configuration server. Upon receiving the encrypted token, the configuration server validates the terminal and identifying token (step 907) and checks if configuration data about the particular terminal is available (step 908). If configuration data intended for the terminal is available, then in step 909, the server authenticates itself to the terminal, for example, by signing data with the private key of server's key pair. This signature is verified by the terminal by using the public key of the server's key pair and comparing the signed data to ensure that it was signed by the corresponding private key which is only known to the server. In step 910, the server signs and/or encrypts at least a portion of the configuration information, and transmits the encrypted and/or signed data to the terminal (step 911).

B5